

PATENT

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

Appellants: Andrew Charles	)	On Appeal to the Board of Appeals
David Hay, <i>et al.</i>	)	
	)	Art Unit.: 2173
Serial No.: 09/931,657	)	
	)	Examiner: Nguyen, Cao H.
Filed: August 16, 2001	)	
	)	Our Ref: B-4271 618992-5
For: "Security apparatus"	)	
	)	Date: March 06, 2008
	)	
		Re: <i>Brief on Appeal</i>

**BRIEF ON APPEAL**

Mail Stop Appeal Brief - Patents  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Dear Sir:

This is an appeal from the Final Action, dated October 15, 2007, for the above identified patent application. The Notice of Appeal was filed on January 08, 2008. Appellants submit that this Appeal Brief is being timely filed before the final deadline of March 7, 2008. Please charge the Appeal Brief fee of \$510 to deposit account no. 08-2025.

**REAL PARTY IN INTEREST**

The real party in interest to the present application is Hewlett-Packard Development Company, LP, a limited partnership established under the laws of

the State of Texas and having a principal place of business at 20555 S.H. 249 Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC.

### **RELATED APPEALS AND INTERFERENCES**

Appellants submit that there are no other prior and pending appeals, interferences or judicial proceedings which may be related to, directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

### **STATUS OF CLAIMS**

Claims 1-17 are currently pending. Claims 1-17 stand rejected and are the subject of this Appeal and are reproduced in the accompanying Claims Appendix.

### **STATUS OF AMENDMENTS**

No Amendment After Final Rejection has been entered.

### **SUMMARY OF CLAIMED SUBJECT MATTER**

The invention described and claimed in the present application relates to security apparatus. The embodiments of security apparatus, computer system and methods for modifying the security status of a computer apparatus are exemplified in independent claims 1, 6, 10, and 14.

The present invention teaches a security apparatus comprising a receiver for receiving a security metric associated with a computer entity; means for presenting to a user the security metric; means for modifying a security setting associated with the computer entity to enable the modification of the security metric associated with the computer entity. Preferably the security metric is presented to a user as a representational model of software and/or hardware functionality of the computer entity. Preferably the security apparatus further comprises input means for allowing a user to interact with the modifying means to modify the security setting. Preferably the security apparatus further comprises means for establishing possible modifications to the security setting based upon the received security metric. Preferably the level of complexity of that which is presented is selectable by a user. (Paragraphs [0006]-[0010] of the present application as published).

Claim 1 of the present disclosure is directed to a security apparatus comprising: means for representing to a user a plurality of components of a computer platform (501; Fig. 6; Paragraph [0061] of the present application as published); means for representing to the user interactions (502, Figs. 5 and 8, paragraphs [0060] and [0065]) among the plurality of components (Figs. 7a-14; Paragraphs [0062]-[0093]); and means for allowing the user to modify a security setting (Paragraphs [0067, 0069-0070], and [0081-0082]) associated with at least one of the plurality of components (Paragraphs [0095]-[0102]).

Claim 6 of the present disclosure is directed to a method for modifying the security status of a computer apparatus, the method comprising: representing to a user a plurality of components of a computer platform (501; Fig. 6; Paragraph

[0061]); representing to the user interactions (502, Figs. 5 and 8, paragraphs [0060] and [0065]) among the plurality of components (components of 501; Figs. 7a-14; Paragraphs [0062]-[0093]); and allowing the user to modify a security setting (Paragraphs [0067, 0069-0070], and [0081-0082]) associated with at least one of the plurality of components (Paragraphs [0095]-[0102]).

Claim 10 of the present disclosure is directed to a computer system, comprising: a memory (22) to store computer-readable code; and a processor (21) operatively coupled to said memory and configured to implement said computer-readable code, said computer-readable code being configured to: represent to a user a plurality of computer components (501; Fig. 6; Paragraph [0061]); represent to the user interactions (502, Figs. 5 and 8, paragraphs [0060] and [0065]) among the plurality of computer components (components of 501; Figs. 7a-14; Paragraphs [0062]-[0093]); and allow the user to modify a security setting (Paragraphs [0067, 0069-0070], and [0081-0082]) associated with at least one of the computer components (Paragraphs [0095]-[0102]).

Claim 14 of the present disclosure is directed to a method for modifying the security status of a computer component, the method comprising: depicting a plurality of computer components (501; Fig. 6; Paragraph [0061]); depicting interactions (502, Figs. 5 and 8, paragraphs [0060] and [0065]) among the plurality of computer components (components of 501; Figs. 7a-14; Paragraphs [0062]-[0093]); and allowing modification of a security setting (Paragraphs [0067, 0069-0070], and [0081-0082]) associated with at least one of the computer components (Paragraphs [0095]-[0102]).

## **GROUND'S OF REJECTION TO BE REVIEWED ON APPEAL**

**Issue 1:** Whether Claims 1-17 are patentable under 35 U.S.C. § 102(b) in view of Calamera, U.S. Patent No. 5,966,441, (hereinafter, Calamera).

## **ARGUMENT**

**Issue 1:** Whether Claims 1-17 are patentable under 35 U.S.C. § 102(b) in view of Calamera, U.S. Patent No. 5,966,441, (hereinafter, Calamera).

In the final Office Action of October 15, 2007, the Examiner rejects Claims 1-17 under 35 U.S.C. 102(b) as being anticipated by Calamera. Appellants respectfully disagree with the Examiner's rejection since the Examiner has not shown that Calamera teaches each and every element set forth in the rejected claims. Appellants request that the rejection be overturned on appeal.

Calamera teaches a technique for creating an autonomous network entity that stores sensitive information in a cryptographically secure manner. The autonomous entity comprises a data structure that encapsulates cryptographically-transformed information along with the inputs of a secret key used to reverse the transformation. Cryptographic storage of the sensitive information and its reversible key within the encapsulated entity makes the entity autonomous and capable of transfer among computer platforms and their

processes without compromising the security of the information. (Calamera Abstract).

Calamera does not disclose, suggest, or teach several features recited in Appellants' claims. In particular:

Claim 1

A. Appellants submit that the Examiner has not shown that Calamera discloses, suggests or teaches, *inter alia*, the following features specifically recited in Claim 1 of the present application:

"means for representing **to a user** a plurality of components of a computer platform" (Emphasis added)

The Examiner asserts that this feature is disclosed by Calamera's teaching that "the computing platform may comprise any network-centric platform that includes a computing device configured to interact with user" (P. 2, section 2, ll. 4-6 of the Office Action). Appellants respectfully traverse the Examiner's assertion.

The Examiner states that he relies on column 5, ll. 53-67 of Calamera for the above quote. However, the Examiner has misquoted what is set forth by Calamera at column 5, ll. 53-67. Calamera really states at column 5, lines 62-64, "The computing platform may ... a computer device configured to interact with a **server**." (Emphasis added). Calamera then teaches a network-centric platform that includes a computing device configured to interact with a **server**, not a network-centric platform that includes a computing device configured to interact

with **a user**, (Column 5, ll. 62-64 of Calamera).

Calamera does not disclose “means for representing **to a user**” as recited in Claim 1. The language relied upon by the Examiner does not teach interaction with a user, it teaches interaction with **a server**.

Appellants submit that the rejection of the Examiner fails to comply with 37 C.F.R. §1.104(c)(2) which states:

“In rejecting claims for want of novelty or for obviousness, the examiner must cite the best references at his or her command. When a reference is complex or shows or describes invention other than that claimed by Appellants, **the particular part relied on must be designated as nearly as practicable**. The pertinence, if not apparent, must be clearly explained and each rejected claim specified” (Emphases added).

The Examiner has failed to “designate as nearly as practicable” where Calamera discloses “means for representing **to a user** a plurality of components of a computer platform” (Emphasis added) as recited in Claim 1.

Because Calamera does not disclose “means for representing to a user a plurality of components of a computer platform” as recited in Claim 1, Claim 1 is patentable over Calamera and the rejection of claim 1 should be overturned on appeal. Claims 2-5, at least based on their dependency on Claim 1, are also patentable over Calamera and should also be allowed.

**Examiner's response to Appellants' arguments:**

On page 5 of the final Action, in the first full paragraph, the Examiner has disagreed with Appellants' argument that Calamera does not teach, "means for representing to a user a plurality of components of a computer platform," as recited in claim 1. He states, "As shown in Figs. 1-2, Calamera teaches the computing platform may comprise any network-centric platform that includes a computing device configured to interact with a server ... as recited in column 5, lines 60-67 [of Calamera]." Appellants respectfully traverse this characterization of Calamera as not correct and request reconsideration and allowance on appeal for the following reasons.

Figs. 1-2 of Calamera do not teach or suggest a user. Both Figs. are being attached with this appeal brief, and listed in the Evidence Appendix, for the convenient reference of the Board. The description of Fig. 2 in Calamera is, "The mouse 230 typically contains at least one button 234 operated by a user of the computer." (Column 6, lines 34-35 of Calamera). In column, 5, lines 64-67, Calamera discloses, "for ease of description and depiction (sic), the computing platform described herein comprise separate client and server computers." That teaching does not anticipate "means for representing to a user a plurality of components of a computer platform" as specifically recited in claim 1. Accordingly, the Appellants request that the Examiner's rejection of claim 1 under 35 USC § 102(b) be overturned.



**B.** Appellants submit that the Examiner has not shown that Calamera discloses, suggests or teaches, *inter alia*, the following features specifically recited in Claim 1 of the present application:

**"means for representing to the user interactions among the plurality of components"** (Emphasis added)

The Examiner seems to assert that this feature is disclosed by Calamera's teaching that "network-oriented component layer contains the underlying technology for creating encapsulated entity components that contain references to network resources located on computer networks" (P. 2, section 2, ll. 7-9 of the Office Action). He directs Appellants to column 8, lines 5-35 of Calamera. Appellants respectfully traverse the Examiner's position.

The language quoted by the Examiner discloses creation of encapsulated entity components that contain references to network resources. But Appellants find no mention that the user is being presented with "interactions among the plurality of components" as recited in Claim 1.

Rather Appellants find that Calamera teaches that the encapsulated entities manifest as visual objects to a user via a window environment to facilitate interactions between the user and the computer (c. 8, ll. 22-27 of Calamera). Calamera does not teach "interactions among the plurality of components" as recited in Claim 1. The only teaching by Calamera of interaction found by Appellants is interaction of network components with system software routines (Column 8, ll. 29-32 of Calamera). This is not "means for representing to the user interactions among the plurality of components" as claimed in claim 1 and

the Examiner seems to rely on Calamera's interaction of network components with system software routines to disclose "interactions among the plurality of components."

The Examiner must comply with 37 C.F.R. §1.104(c)(2) and "designate[d] as nearly as practicable" where Calamera teaches "means for representing to the user interactions among the plurality of components," as claimed in claim 1. Given the fact that the Appellants cannot find such designation, the Examiner has not complied.

Because Calamera does not teach "means for representing to the user interactions among the plurality of components," as recited in claim 1, Calamera does not teach, disclose or suggest such means. Claim 1 is, therefore, patentable over Calamera the rejection of claim 1 under 35 USC § 102(b) should be overturned. Claims 2-5, at least based on their dependency on Claim 1, are also patentable over Calamera and their rejection should be reversed on appeal.

**Examiner's response to Appellants' arguments:**

On page 5 of the final Action, in the second full paragraph, lines 2-3, the Examiner seems to have stated that the feature "means for representing to the user interactions among the plurality of components," as recited in Appellants' claim 1, is taught by Calamera. He states, "... suggest represent to a user a plurality of computer components, represent to the user interactions among the plurality of computer components." Appellants respectfully traverse and request reconsideration and allowance of claim 1.

Figs. 2-5 of Calamera do not teach or suggest a user. Fig. 2 is a block diagram of a client computer, such as a personal computer, on which the invention may advantageously operate; Fig. 3 is a block diagram of the server computer of Fig. 1; Fig. 4 is a highly schematized block diagram of a layered component computing arrangement in accordance with the invention; and Fig. 5 is a schematic illustration of the interaction of a component, a software component layer and an operating system of the computer of Fig. 2. (Calamera Brief Description of the Drawings).

In column 8, lines 17-24, where the Examiner has directed Appellants, Calamera discloses, “[t]he network-oriented component system which, when invoked, causes actions to take place that enhance the ability of a user to interact with the computer to create encapsulated entities that contain references to network resources located on computer networks, such as the Internet.” This disclosure does not teach or suggest the feature “means for representing to the user interactions among the plurality of components” specifically recited in claim 1. Something may “enhance the ability of a user to interact with the computer” but this is not “means for representing to the user interactions among the plurality of components.” Moreover, Calamera discloses, “This behavior of the system is brought about by the interaction of the network components with a series of system software routines associated with the operating system 420. These system routines, in turn, interact with the component architecture layer 430 to create the windows and graphical user interface elements” (c. 8, ll. 28-33 of Calamera). This is the language the Examiner cites as anticipating of claim 1. This language does not teach or suggest “means for representing to the user

interactions among the plurality of components” as recited in claim 1. Accordingly, the Appellants request that the Examiner’s rejection of claim 1 be overturned.

C. Appellants submit that the Examiner has not shown that Calamera discloses, suggests or teaches, *inter alia*, the following features specifically recited in Claim 1 of the present application:

“means for **allowing the user to modify a security setting** associated with at least one of the plurality of components”  
(Emphasis added)

The Examiner asserts that this feature is disclosed by Calamera at column 12, ll. 21-51 (P. 2, section 2, ll. 9-11 of the Office Action). Appellants respectfully traverse the Examiner’s assertion.

Although Calamera’s column 12, ll. 21-51, relied upon by the Examiner discloses associating information securely with the encapsulated network entity, Appellants submit that Calamera’s column 12, ll. 21-51, does not disclose “allowing the user to modify a security setting” as recited in Claim 1. According to the portion of Calamera text relied upon by the Examiner, Calamera creates an autonomous network entity that stores sensitive information in a cryptographically secure manner (C. 12, ll. 25-28 of Calamera). The Examiner has failed to show where Calamera teaches that this autonomous network entity allows “the user to modify a security setting” as recited in Claim 1.

Appellants again submit that the Examiner has not complied with 37 C.F.R. §1.104(c)(2). He has not designated “as nearly as practicable” where Calamera

teaches that the user is allowed to “modify a security setting” as recited in Claim 1.

Because Calamera does not allow the user to “modify a security setting” as recited in Claim 1, Claim 1 is patentable over Calamera and the rejection of claim 1 should be overturned on appeal.

Claims 2-5, at least based on their dependency on Claim 1, are also patentable over Calamera and their rejection should be overturned on appeal.

**Examiner’s response to Appellants’ arguments:**

On page 6 of the final Action, in the first full paragraph, the Examiner has disagreed with Appellants’ argument that Calamera does not teach “means for allowing the user to modify a security setting associated with at least one of the plurality of components,” as recited in claim 1. Appellants respectfully traverse and request reconsideration and allowance on appeal for the following reasons.

According to the Examiner, in Figs. 10-11, Calamera teaches “The viewing editor 660 then modifies or displays, either visually or acoustically, the contents of the data types. The window object 630 and the graphic interface object 650 are elements of a graphical user interface of a network component system that greatly enhances the ability of a user to efficiently access information from a network resource on computer networks by creating an encapsulated entity that contains a reference to that resource. The encapsulated entity is preferably implemented as a network component of the system and stored as a visual object, e.g., an icon, for display on a graphical user interface. Such visual display

allows a user to easily manipulate the entity component to display the contents of the resource on a computer screen or to electronically forward the entity over the networks." The appellants respectfully traverse.

To begin with, Figs. 10-11 of Calamera do not teach or suggest a user. In column, 10, lines 31-45, Calamera does disclose,

"The viewing editor 660 then modifies or displays, either visually or acoustically, the contents of the data types.

The window object 630 and the graphic interface object 650 are elements of a graphical user interface of a network component system that greatly enhances the ability of a user to efficiently access information from a network resource on computer networks by creating an encapsulated entity that contains a reference to that resource. The encapsulated entity is preferably implemented as a network component of the system and stored as a visual object, e.g., an icon, for display on a graphical user interface. Such visual display allows a user to easily manipulate the entity component to display the contents of the resource on a computer screen or to electronically forward the entity over the networks."

but that disclosure does not anticipate "means for allowing the user to modify a security setting associated with at least one of the plurality of components." as recited in claim 1. The text cited by the Examiner (Column 10, lines 3-57) is a description of Fig. 6 of Calamera which is merely a schematic illustration of the interaction between a component, a component layer and a window manager, nowhere disclosing "allowing the user to modify a security

setting," for example. Accordingly, the Appellants request that the Examiner's disagreement be overturned on appeal.

#### Claim 6

Appellants submit that, at least for the reasons stated above for Claim 1, Calamera does not teach, disclose or suggest "**representing to a user** a plurality of components of a computer platform; representing to the user **interactions among the plurality of components**; and **allowing the user to modify a security setting** associated with at least one of the plurality of components" (Emphases added) as recited in Claim 6. Hence, Claim 6 is patentable over Calamera and the rejection of claim 6 should be overturned on appeal. Claims 7-9, at least based on their dependency on Claim 6, are also patentable over Calamera and their rejection should be overturned on appeal.

#### Claim 10

Appellants submit that, at least for the reasons stated above for Claim 1, Calamera does not teach, disclose or suggest "**represent to a user** a plurality of computer components; represent to the user **interactions among the plurality of computer components**; and **allow the user to modify a security setting** associated with at least one of the computer components" (Emphases added) as recited in Claim 10. Hence, Claim 10 is patentable over Calamera and the rejection of claim 10 should be overturned on appeal. Claims 11-13, at least based on their dependency on Claim 10, are also patentable over Calamera and their rejection should be overturned on appeal.

Claim 14

Appellants submit that, at least for the reasons stated above for Claim 1, Calamera does not teach, disclose or suggest “**depicting interactions among the plurality of computer components; and allowing modification of a security setting** associated with at least one of the computer components” (Emphases added) as recited in Claim 14. Hence, Claim 14 is patentable over Calamera and the rejection of claim 14 should be overturned on appeal. Claims 15-17, at least based on their dependency on Claim 14, are also patentable over Calamera and their rejection should be overturned on appeal.



### CONCLUSION

For the reasons advanced above, Appellants respectfully contend that each claim is patentable. Therefore, reversal of all rejections is courteously solicited.

The Commissioner is authorized to charge any additional fees, which may be required or credit overpayment to deposit account no. 08-2025. In particular, if this response is not timely filed, then the Commissioner is authorized to treat this response as including a petition to extend the time period pursuant to 37 CFR § 1.136 (a) requesting an extension of time of the number of months necessary to make this response timely filed and the petition fee due in connection therewith may be charged to deposit account no. 08-2025.

I hereby certify that this correspondence is being transmitted to the United States Patent and Trademark Office via electronic filing on

March 06, 2008  
(Date of Transmittance)

Krista Celentano  
(Name of Person Transmitting)

/Krista Celentano/  
Signature

Respectfully submitted,

/Amit Singh/  
Amit Singh  
Attorney for Appellants  
Reg. No. 54451  
LADAS & PARRY  
5670 Wilshire Blvd., Suite 2100  
Los Angeles, CA 90036  
(323)934-2300

1. Security apparatus comprising:

means for representing to a user a plurality of components of a computer platform;

means for representing to the user interactions among the plurality of components;

and

means for allowing the user to modify a security setting associated with at least one of the plurality of components.

2. Security apparatus according to claim 1, wherein the means for representing the plurality of components comprise: means for representing software and/or hardware functionality of the computer platform.

3. Security apparatus according to claim 1, further comprising input means for allowing the user to interact with the modifying means to modify the security setting.

4. Security apparatus according to claim 1, further comprising means for providing possible modifications to the security setting.

5. Security apparatus according to claim 1, wherein a level of complexity of representing to the user the plurality of components is selectable by the user.

6. Method for modifying the security status of a computer apparatus, the method

comprising:--

- representing to a user a plurality of components of a computer platform;
- representing to the user interactions among the plurality of components; and
- allowing the user to modify a security setting associated with at least one of the plurality of components.

7. The method according to claim 6, wherein representing the plurality of components comprises:

- representing software and/or hardware functionality of the computer platform.

8. The method according to claim 6, further comprising:

- presenting to the user possible modifications to the security setting.

9. The method according to claim 6, further comprising:

- allowing the user to select a level of complexity of representing to the user the plurality of components.

10. A computer system, comprising:

- a memory to store computer-readable code; and
- a processor operatively coupled to said memory and configured to implement said computer-readable code, said computer-readable code being configured to:
  - represent to a user a plurality of computer components;
  - represent to the user interactions among the plurality of computer components; and
  - allow the user to modify a security setting associated with at least one of the

computer components.

11. The computer system according to claim 10, wherein representing the plurality of computer components comprises:

representing software and/or hardware functionality of a computer.

12. The computer system according to claim 10, wherein the computer-readable code is further configured to:

present the user possible modifications to the security setting.

13. The computer system according to claim 10, wherein the computer-readable code is further configured to:

allow the user to select a level of complexity of representing to the user the plurality of computer components.

14. Method for modifying the security status of a computer component, the method comprising:-

depicting a plurality of computer components;

depicting interactions among the plurality of computer components; and

allowing modification of a security setting associated with at least one of the computer components.

15. The method according to claim 14, wherein depicting the plurality of computer

components comprises:

depicting software and/or hardware functionality of a computer.

16. The method according to claim 14, further comprising:

presenting possible modifications to the security setting associated with one or more of the computer components.

17. The method according to claim 14, further comprising:

allowing selection of a level of complexity for displaying the plurality of computer components.

## **Evidence Appendix**

Figs. 1-2 of Calamera.

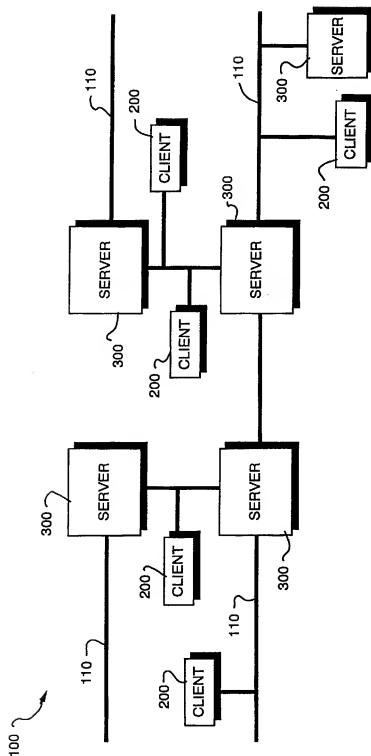


FIG. 1

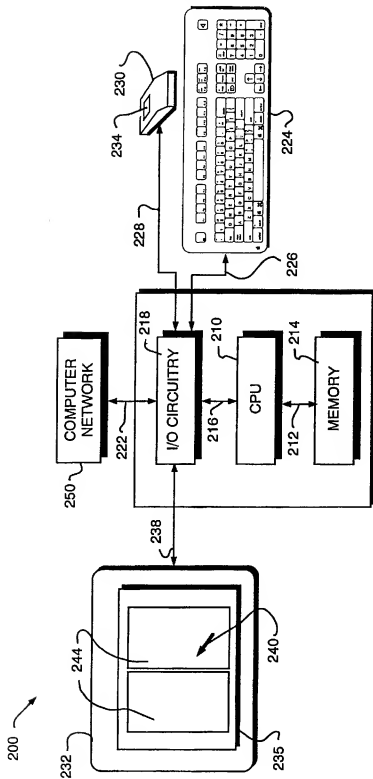


FIG. 2



**Related Proceedings Appendix**

No copies of decisions rendered in related proceedings are being submitted.